REMARKS

The Applicants request reconsideration of the final rejection dated January 28, 2008.

Claims 1-8 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the Applicants' admitted prior art in view of Jaffe et al., U.S. Patent No. 6,510,518 (Jaffe). Although the Applicants continue to assert that the claims, as finally rejection, were patentably distinguishable from the admitted prior art in view of Jaffe for reasons set forth in previous responses, in an attempt to advance the application to issue, and resolve matters of dispute, claim 1 has been amended to limit the operation, and therefore the structure, of the claimed data transform means such that the data transform means transforms the input data D1 which does not have a constant Hamming weight, by using disturbance data XI having a constant hamming weight, to generate the transformed data H1. The distinction further distinguishes Jaffe, which discloses in col. 4, lines 58-59 that "Operations are performed using a data representation such that the Hamming weight of all input values is constant." By requiring that the Hamming weight of all input values be constant, Jaffe requires the number of bits of the input data to necessarily increase in number. Consequently, the circuit inputting and transforming the data according to Jaffe increases in scale or size correspondingly.

On the other hand, the now-claimed invention has a constant Hamming weight only for the disturbance data, and does not require the input data to have a constant Hamming weight. Indeed, as amended, claim 1 requires the input data D1 to <u>not</u> have a constant Hamming weight.

Claims 18-22 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for the reasons set forth on page 7 of the Office Action. Claims 18 and 21 have been amended to address each of the Examiner's concerns.

Claims 1-8 and 18-22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the admitted prior art in view of Jaffe. Claims 1-8 have been distinguished above; claims 18-22 are distinguished below.

As amended, claim 18 requires the processor to concatenate a predetermined number of m-bit random numbers randomly into first disturbance data of n-bits equal to a multiple of m. The processor is no longer recited as performing the generation of m-bit random numbers having a predetermined Hamming weight, or processing the first disturbance data with a first operation, generating second disturbance data, and evaluating whether the second disturbance data has a target Hamming weight. Rather, the processor is now recited as being arranged to transform input data into first transformed data with the first disturbance data, process the first transformed data with a first operation, generate second transformed data, process the first disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data with the second disturbance data. Jaffe is not seen, at least, to perform this latter inverse-transform using the second disturbance data.

New claims 23-26 are also patentably distinguishable from the art of record, whether taken individually or in any reasonable combination. In particular, claim 23 recites an information processing apparatus comprising a processor, a storage, and a data bus, wherein the processor is arranged to transform input data into first transformed data with first disturbance data, process the first transformed data with a

first operation, generate second transformed data, process the first disturbance data with the first operation, generate second disturbance data, and inverse-transform the second transformed data into processed data with the second disturbance data. Thus, as argued above with regard to claim 18, claim 23 is patentably distinguishable from the admitted prior art in view of Jaffe, at least in regards to the step of inverse-transforming the second transformed data into processed data with the second disturbance data.

The separate patentability of the dependent claims will not be argued at this time, for brevity. However, the Applicants retain the right to all subject matter as claimed.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. NIT-295).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

_____/Daniel J. Stanger/_____
Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1120

11